A POLICY MECHANISM FOR FEDERAL RECOMMENDATION OF SECURITY STANDARDS FOR MOBILE DEVICES THAT CONDUCT TRANSACTIONS

A Thesis

Presented to

the Faculty of the Daniel Felix Ritchie School of Engineering and Computer Science

University of Denver

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

---

by

Ariel Huckabay

November 2019

Advisor: Dr. Scott Leutenegger

Author: Ariel Huckabay
Title: A POLICY MECHANISM FOR FEDERAL RECOMMENDATION OF SECURITY STANDARDS FOR MOBILE DEVICES THAT CONDUCT TRANSACTIONS
Advisor: Dr. Scott Leutenegger
Degree Date: November 2019

ABSTRACT

The proliferation of mobile devices in the BRIC countries has prompted them to develop policies to manage the security of these devices. In China, mobile devices are a primary tool for payments. As a result, China instituted in 2017 a cyber security policy that applies to mobile devices giving China broad authority to manage cyber threats. The United States has a similar need for a cyber policy. Mobile devices are likely to become a primary payment tool in the United States soon. DHS has also identified a need for more effective security policy in mobile devices for government operations. This work proposes a certification program for mobile devices that can achieve the same level of security as China's policy without the threats to privacy and intellectual property. It will also afford the United States a more authoritative position to shape global cyber norms as cyberspace evolves.

Table of Contents

Introduction

Introductory Chapter

The proliferation of mobile devices in the BRIC countries has prompted significant thought and policymaking with respect to mobile device security in the developed and developing world alike. In the BRICS Countries, Brazil, Russia, India, China, and South Africa (since 2011), their position on the world stage is moving toward being among the countries that set precedents for international law and the countries that lead multilateral actions. China has instituted their Network Security Act of the People's Republic of China, for example, which outlines rights of the government to take nearly any action deemed to be necessary to protect the 'societal public interest,' including access to source code. This Act was implemented following the tremendous increase in the use of mobile devices capable of financial transactions. This increase constitutes significant growth in the size of the front of vulnerability to a cyberattack. While China's Act provides a unique legal framework for responding to cyber threats, it does not outline a specific method by which devices can be developed more securely or have improved security in operation. Furthermore, the reach of that law is well beyond what would comport with the United States Constitution.

The developed world has adopted mobile devices for payment at a slower rate. As a result, there has been less dialogue regarding how to create a national security standard for these devices. The rate of adoption of mobile devices and other ‘internet of things’ devices, as well as cyber incidents in the BRICS countries, is prompting discussion of their own respective cyber policies. While their policies are not directly adoptable by the United States, they do provide a reference point for developing a policy in the United States with similar purposes.

This work will argue that the data on mobile transactions in the United States shows that its insecurity represents a substantial economic cost worthy of being ameliorated. It will then outline and analyze the implications of the cyber policies or policy proposals in the BRICS countries, with particular emphasis on China’s. Finally, it will propose a policy mechanism for the United States that could accomplish the same security standards without the same degree of risk to intellectual property that more severe policies pose and be within the bounds of United States law.

Chapter 1 will discuss the data on the adoption of mobile payments in the United States to show the rate of the growth of the surface area of vulnerability. It will argue that the number is likely to become significant enough that the security of these devices must be taken seriously. Chapter 2 will discuss the policies already implemented and those currently in development in Brazil, India, and China. In the countries of Russia and South Africa, their policies are not as well developed and therefore are not as useful to analyze for this purpose. Chapter 2

will also explain the motivations and scope of each law. Chapter 3 will propose a certification program that the United States could implement to standardize security rules for mobile devices. It will also discuss the potential benefits of this program, including overcoming barriers to adopting mobile devices as primary forms of payment.

This certification program will allow the United States to avoid the appearance of bestowing an advantage on domestic businesses over foreign ones in recommending security principles. This, in turn, will put the United States in a better position to shape cyber-norms. A certification program would require voluntary private-sector participation to be effective. One barrier to the adoption of mobile payments in the United States has been perceptions that credit cards are more secure than mobile payments. This policy could also help to change that perception by demonstrating that security is a priority for technology companies as well as the government in a time when personal data is frequently compromised.

Mobile transactions are defined as any transaction conducted using a mobile device. Mobile transactions are increasing in dollar amount and frequency along with most forms of payment according to the Federal Reserve Payments Survey. Checks are the only form of payment on the decline. Despite their growth, mobile payments still represent a small portion of all payments in the United States. The barriers to more widespread adoption are declining due to improving perceptions of their security, faster adoption among younger

consumers, and an increase in retailers and restaurants accepting mobile payments. In 2014, only 3% of retailers accepted Apple Pay, but by 2018, 50% did according to eMarketer, a market research firm. The perceptions of security concerns are being combatted through advertising. Additionally, younger consumers (18-35) are much more likely to use and trust mobile payments, as reported in the Economist. This group of users makes up roughly 40% of the working population currently [Brookings, 2018]. Assuming generations following this one are similarly apt to use mobile payments, the vast majority of the workforce will be accustomed to mobile payments as a main form of payment by 2050, using projections reported by the Pew Research Center. At present, the global mobile payments market is over $3 trillion USD. Assuming consumers continue to use mobile payments at current rates, mobile transactions are likely eventually to represent a multi-trillion-dollar portion of domestic consumption, and mobile devices will likely be a primary location for sensitive financial information. Mobile payments will only account for under 2% of all retail and restaurant transactions in 2019 according to a Forbes estimate. Given their projected growth, it is an ideal time to implement a policy to manage security standards for these devices in preparation for their more widespread adoption.

Mobile payments have already reached wide-spread adoption in China and are being rapidly embraced in the rest of the developing world. This is likely due to the technology available at their stage of economic development. The same payment systems that are available in the United States, such as PayPal

and Apple Pay, are available or soon to become available in Brazil, India, and China. Consequently, the security concerns that their policies are designed to mitigate will need to be addressed in the United States by the time mobile transactions reach widespread adoption.

China's network security law, The Network Security Act of the People's Republic of China, essentially states that it has the right to any information about any devices that run on any network inside China. This includes source code. This represents a significant risk to intellectual property for any company doing business inside China. The motivation for this approach seems to be ensuring that security interests supersede any others when vulnerabilities are discovered. Brazil and India prioritize privacy in their laws, which are much more akin to the European Union's General Data Privacy Regulation (GDPR). They rely on the public-private partnership between firms and seek to conform to international norms on data privacy.

The relative positions of China, the European Union, Brazil, and India help to explain the priorities of their cybersecurity laws. China is positioned as a rising economic power through the development of their financial sector, technology sector, and through expanding their military. The other listed countries fall under the security umbrella of the United States. While privacy is not unimportant in the United States, security is of much greater concern to China, and must be the priority in a cyber policy that the United States adopts as well. China operates as a regional hegemon with security priorities that often clash with those of United

States and its allies. While policies in the spirit of the GDPR are aimed at mitigating exploitation of personally identifiable information for financial gain, China's policy is as oriented toward mitigating threats from state actors as much as criminals and other non-state actors. The United States as a hegemon must focus on this as well. The United States cannot adopt the heavy-handed approach of China within its legal boundaries. This means that the United States requires significant participation from the makers of mobile devices to achieve similar security objectives. It must leverage natural incentives to protect users of mobile devices from threats originating from the exploitation of personal data as well as from adversarial states. The certification program proposed in this work can achieve these goals.

The certification program would require compliance with a set of security recommendations that can be updated to counter newly discovered threats or resolve emergent vulnerabilities. As a beginning point, this work recommends implementing the 10 controls described in Cavallari et al and forcing software updates to be applied automatically within a certain timeframe. The goal will be to prevent users from rooting their devices and in so doing potentially removing protections or avoiding critical security updates. The security standards that appear in this set should be:

1) Targeted at a specific security threat or vulnerability rather than the origin of hardware

2) Addressable by mobile device creators through patches or updated hardware in new devices
3) Solution and business-goal agnostic

This approach to mobile device security is beneficial to consumers by creating a metric for security that can serve as a basis for competition between mobile devices. It is beneficial to the creators of mobile devices by incentivizing users to upgrade their phones regularly to avoid using devices with outdated security capabilities. From a domestic standpoint, this approach is compatible with consumer protection as well as business motivations.

Internationally, the United States has struggled at times to rally sufficient soft power to advocate against devices or infrastructure developed by non-United States entities. Huawei is the most pronounced example. While the United States has insisted that Huawei hardware should not be used in our mobile networks and that any hardware created in China be removed from United States Government systems, other countries (notably, the other 'Five-Eyes' countries) did not immediately find the concerns voiced by the United States as compelling. Huawei owns a larger portion of 5G related patents than companies in the United States and has argued that the United States is trying to advantage its domestic businesses under the guise of security. A formalized mechanism to recommend security standards that are based only on security strengthens the position to advocate for policies that happen to go against the interests of a particular mobile device creator, be they foreign or domestic.

The proposed policy can improve the ability of the United States to respond to security concerns in the mobile space and influence norms toward particular security standards. It accomplishes much of what China's policy can accomplish without compromising intellectual property. It will also facilitate the United States' advocacy of security standards to comport with a model of the acceptable use of cyberspace as it is developed in the international community.

Chapter 1: The Adoption of Mobile Devices in the United States

Introduction

Mobile devices have not yet become a primary tool for consumer spending. Perceptions over their security and consumer habits around credit cards in the United States seem to be hindering the rate of mobile payment adoption for retailers and restaurants [Economist, 2018]. However, mobile devices are useful for remote payments as well as in-person payments at restaurants and retailers. Consequently, the overall usage of mobile payments is growing without yet replacing credit cards for retail. An estimate from Forbes finds that mobile payments will account for under 2% of all mobile retail and restaurant consumption in 2019. However, the total amount of money involved in transactions conducted by mobile devices is projected to be over $141 billion for 2019 [Statista, 2015]. Other projections are similar. If mobile devices become the primary tool for in-person retail and restaurant payments as well as remote payments and peer-to-peer transfers, then the measures to keep these devices secure will be much more important. This day is likely to come.

There are three main barriers to transactions conducted via mobile devices becoming as common or more common than credit and debit cards. The first is that retailers and restaurants are generally equipped for credit cards but are not equipped for mobile payments. The second is that there is a perception that credit and debit cards are more secure than mobile payments. They are not; why they are not will be discussed in Chapter 3. The third is simply that the largest group of consumers is simply more accustomed to credit and debit cards and they have no clear incentive to change this.

This section will show that these barriers are each being overcome and that current adoption trends are likely to lead to mobile devices overtaking credit and debit cards as the primary forms of payment for remote payments, peer-to-peer transfers, and in-person retail and restaurant purchases. The first barrier is being overcome through various technology companies innovating cost-effective solutions for businesses to adopt. While a large portion of retailers still do not accept mobile payments, the proportion that do has grown rapidly, and continues to grow. The second and third barriers are somewhat intertwined. The perceptions over the insecurity of mobile devices are being combated through marketing and innovation, though it is younger consumers (18-35) that seem to be most receptive to this message. Similarly, while this portion of consumers account for less than half of all consumption, they are much more in the habit of using mobile payments according to surveys reported by the Economist.

Consequently, as this set of consumers grows in proportion of consumption, mobile payments will grow along with them.

This section will also discuss data on China's, India's, and Brazil's adoption of mobile devices to provide context to the mobile payment ecosystem and the conditions under which each of these countries chose to implement their respective cybersecurity laws.

Mobile Payment Options and Payment Trends

United States

Support for mobile payment options in retail and restaurants are being adopted rapidly, with Apple Pay leading the charge. Even though mobile payments still do not account for a very large portion of retail sales, their availability is growing rapidly. It is possible that at present this is no longer a barrier to the adoption of mobile payments over credit and debit cards, though it does slow down the rate of adoption. Trends from the Federal Reserve Payments Study 2018 show that checks are on the decline while all other forms of payment are increasing as overall consumption has been increasing.

In 2014, Apple Pay launched, and was accepted by 3% of retailers. In 2017, only 36% of retailers accepted any form of mobile payment [Forester Research, Inc., 2017]. In 2018, Apple Pay was an option at 50% of retailers and restaurants and in 2019, Apple claimed that that number is now 65%. More than 80% of retailers support or intended to support Apple Pay and 73% support or

intended to support Google Pay by December of 2018 [Boston Retail Partners, 2019]. Other, less popular options include Samsung Pay, Pay Pal, Chase Pay, and branded payment services such as Starbucks.

In addition to retail, mobile payments are used for peer-to-peer transfers and remote payments. Remote payments are by far the largest portion of payments made by mobile devices, projected to be worth an estimated $90.6 billion in 2019 [Statista, 2015]. This is more than double the number from 2014. Peer-to-peer transfers are the smallest segment, projected to be worth around $16.8 billion in 2019.

For the most part, mobile payment services have been adopted sufficiently so that they can be used to perform the same functions as credit cards, debit cards, cash, and checks. While there are still retailers and restaurants at which mobile payment services are unavailable, the number who do not appears to be shrinking rapidly. Nonetheless, mobile payments are not representing a large portion of retail commerce. If the lack of availability of mobile payment support is a barrier to their adoption, it soon will not be.

China

China never chose to adopt credit and debit cards as primary forms of payment. By the point in their economic development at which average consumers were well empowered to consume, mobile technology was largely available and so mobile payments were a natural choice. In 2016, China’s mobile

payments constituted $5.5 trillion in amount and 125 billion in quantity [Financial Times, 2017]. In 2018, roughly 83% of all transactions in China were made via mobile devices [Daxue Consulting, 2019]. The year-over-year growth is, as would be expected, reaching a plateau. Even in rural China mobile payments have significant penetration, with about 47% of residents in rural China regularly utilizing mobile payments [Daxue Consulting, 2019].

To achieve this level of frequency at retailers as well as independent vendors, mobile payment services in China utilize Quick Response (QR) codes regularly. The most prevalent mobile payment services in 2019 are Tenpay (which includes WeChat Pay and QQ Wallet) and AliPay. Apple Pay has not reached the same level of utilization. The struggle of Apple Pay might be due to the fact that retailers need to purchase additional technology to facilitate Near Field Communication (NFC) transactions. With QR codes, the buyer can simply scan the seller's code, or the seller can scan the code for the buyer's mobile wallet and select the amount to charge against the wallet [Daxue Consulting, 2019]. Android has higher penetration in China than Apple, which may also contribute to Apple's struggle. However, Samsung Pay and Google Pay (formerly Android Pay) are not as prevalent either. Domestic payment services are significantly more utilized than foreign-developed ones. China remains the country with the highest level of mobile payment utilization in Asia.

India

India does not use mobile payments to the degree that China does, but it seems to be poised to adopt them at a rate similar to China in the near future. Like China, India is skipping the adoption of credit and debit cards as a means of payment. India is developing mobile payment infrastructure rapidly and the demonetization of their higher-denomination currency has provided an incentive for the adoption of mobile payments. India is the fastest growing mobile payments market. Between 2017 and 2018 there was a 39.7% increase in the number of people using mobile payments, and the trend is expected to continue in 2019 [Kats, 2018].

India is implementing the Universal Payments Interface (UPI) developed by the National Payment Corporation of India. UPI is intended to make mobile devices as efficient a tool for payments as possible. It uses QR codes, like China's payment services, allows consumers and merchants to initiate transactions, and avoids the need for new hardware development.

The largest payment service in India is the Indian-developed Paytm, but foreign-created payment services are also seeking penetration into India's market [Sengupta, 2019]. It is growing rapidly but has not matured to the level of China's.

Brazil

Brazil has a less mature market for mobile payments than China or India but is leading Latin America both in adoption of mobile payments and in mobile payment innovation [Visa Innovation Center, 2019]. Brazil's approach is unique in the BRIC countries and very much tied to their economic position in Latin America. Brazil will have an estimated 141.6 million mobile phone users in 2019, representing a little bit less than 70% of the population, demonstrating significant growth over the last few years [eMarketer and AP, 2015]. Roughly 70% of Brazilians were banked in 2017, but this only represented a small amount of growth from the previous year [World Bank, 2018]. In the context of the number of banked people, Brazil is focusing on making payments easier with their financial technology (fintech) innovations including mobile devices to bring more of the population into the banking system. For Brazil, mobile payment technology is also a means to help those who are banked utilize these technologies more. It is expected that mobile phone penetration will outpace banking penetration. As a result, mobile wallets, wherein electronic money is loaded using cash, offers a means for Brazilians to access some financial services without needing to be banked. While mobile payments have not reached the level of India much less China, they are poised to grow rapidly, and Brazil has prepared for this through new technologies as well as mobile device cybersecurity policy.

Perceptions over Security for Mobile Devices in the United States

One reason reported by consumers in the United States for choosing not to utilize mobile payment services is that they believe they are less secure than card payments [Economist, 2018]. In addition to this, in 2015 a survey published by ISACA of 900 cybersecurity experts from around the world showed that a large majority of 87% of them believed that mobile payment breaches were going to increase in the following year. Their concerns were mainly with respect to using public WIFI when making payments or transmitting related data, lost or stolen devices, and phishing. Despite these concerns, 42% of them had in fact engaged in mobile transactions that year. With the right education and understanding of mobile device security, users can mitigate these concerns with relative ease.

Perceptions of mobile devices being less secure than traditional forms of payment is somewhat self-fulfilling. If mobile devices are perceived to be less secure than their more traditional payment counterparts, then it is more difficult to cultivate a culture of security around them because there is less reason to use mobile devices for payments. The 2015 ISACA survey found respondents agreed that teaching teenagers and potentially younger users of mobile devices to use them effectively would help to alleviate this.

In the United States, the Deloitte 2016 Global Mobile Consumer Survey showed that the belief that mobile devices were not sufficiently secure to be used for payments dropped from 54% of respondents in 2015 to 40% in 2016. Deloitte

reported in 2018 that this had climbed to 42%, tied with a perceived lack of benefit of using them over cards. However, the perceived benefits of using mobile devices for payments increased among consumers who had used mobile payments [Holm et al, 2018]. As Deloitte notes, it is not the case that cards are more secure than mobile devices for payments. As users adopt them, the common understanding of their benefits should become adopted as well.

In Sum

Mobile devices are being used for mobile payments at greater frequency. The United States has a high level of banking and mobile device penetration, but credit and debit cards account for the preponderance of payments. There are three barriers preventing mobile devices from gaining wider adoption as a means of payment. The first is a slow pace of retailers and restaurants adopting the technology to provide mobile payment services. The second is that the belief that they are not as secure as credit and debit cards is reducing consumers' perceived benefit from adopting mobile payments. The third, which is closely related to the second, is that consumers habitually use credit and debit cards and are resistant to adopt a new technology, since to many of them there is no compelling reason to make this change.

Surveys of consumer behavior and perceptions around mobile devices show that consumers who utilize mobile payments are far more likely to perceive a benefit over credit and debit cards and that younger consumers, who are projected to account for roughly 40% of consumers in 2020 are particularly more

likely to utilize mobile payments. Therefore, mobile payments in the United States are likely to grow in popularity with consumers as opposed to cards and represent a much more substantial portion of consumers in the short-term.

Adopting the technologies that allow consumers to use mobile payments is still more difficult for retailers in the United States than it would be in India or China due to the variety of competing services that tend to keep a measure of exclusivity on these services. India has developed the Universal Payments Interface and China's payment services utilize Quick Response codes to make it as easy as possible to unify digital payment services and reduce the cost to retailers and restaurants. Though the United States has not done either of these, there are growing partnerships among mobile payment service providers, and the current Point of Sale technologies accommodate all of the major payment services. This is more expensive for restaurants and retailers, but nonetheless does not prevent the adoption of mobile payments in the United States.

China represents a mature state of mobile payments as a main tool of consumption. India is following closely behind, with some unique motivators to incentivize adopting mobile devices. In particular, India has an underbanked population with high mobile device penetration and demonetization of their higher-denomination currency. Brazil is using mobile technologies to improve banking penetration and is poised to have consumers using digital payments primarily once they are positioned to utilize the financial services that are becoming available. The United States, as an already developed economy, is

moving in this direction slowly but steadily. Mobile payments are most likely going to be a primary payment method in all of these economies in the near future.

Chapter 2: Cybersecurity Policies in Brazil, India, and China

Introduction

Brazil, India, and China are all countries where mobile payments are being adopted rapidly. China represents a mature market for mobile payments, India follows closely behind, and Brazil is poised to adopt as rapidly as India in the near future. In response to these new realities, these three countries are experimenting with cybersecurity policies that apply to mobile devices. There are two distinct approaches in their policies and policy initiatives. China has adopted the Network Security Act of the People's Republic of China, taking an authoritative approach that lists potentially severe actions China might take to resolve a security concern. Brazil and India are prioritizing data privacy and consumer protection in their policies. This is more akin to the European Union's General Data Privacy Regulation (GDPR). For India and Brazil, mobile payments are a tool that can help to provide their underbanked populations access to financial services that are not currently available to them.

China's approach is authoritative, centralized, and broad. China must mitigate threats from cyber criminals as well as from states, and so a security-focused approach that fits within China's authoritative policy structure makes sense. Brazil and India have not instituted policies that are as comprehensive as

China's, but they are preparing to do so. They are primarily focused on fraud and cybercrime, though India is also preparing to mitigate state-level attacks through a more security-focused approach than Brazil.

Brazil has instituted its Online Bill of Rights, Marco Civil da Internet (MCI) to manage privacy standards and developed additional agencies to manage growing cybersecurity threats. These threats take the form of the growing number of cyber incidents in Brazil and Brazil's hosting of more events. India has a cybersecurity policy that has been in place since 2013 and they are expected to launch another one in 2020. They also have a data privacy law that is weaker than GDPR that has been in place since 2011. Now that GDPR is in full effect, India is likely to adopt an updated data privacy policy in the near future.

Brazil's Cybersecurity Policy

The increase in cyber incidents in Brazil has prompted Brazil to include cyber defense in their national defense strategy [Bolzan de Rezende et al, 2018]. In 2014, there were over 1 million cyber incidents, nearly triple the number from the previous year. The number of cyber incidents dropped between 2014, and 2017, but nonetheless, each year since 2014 has seen more cyber incidents than any year before 2014. Geopolitically, Brazil does not face any significant state-level threats, but the perceptions around cybercrime could undercut their efforts to increase the availability of financial services to the Brazilian population.

Though Brazil is more focused on cybercrime than state-level threats, it is developing its increased capabilities to counter cyber threats within their military. Brazil has created the Cyber Defense Command to handle the development of their new capabilities. This suggests that Brazil is anticipating the possibility of mitigating state-level cyber attacks as well as transnational organized cybercrime.

Nonetheless, from a policy perspective, Brazil adopted the Online Bill of Rights in 2013, which is referred to as the Marco Civil da Internet (MCI). This legislation contained 10 guidelines for internet governance [Arnaudo, 2016]:

1) Freedom, privacy and human rights
    - This legislation asserts that the same principle of human rights that are discussed in other arenas are applicable to cyberspace.
    - The right to privacy defined in the law essentially guarantees that a citizen's communications through the internet are secret except for when they are requested by a court order.
2) Democratic and collaborative governance
    - As a reflection of this principle, several Brazilian agencies have online portals to solicit input from private citizens on internet-related governance.
3) Universality

4) Diversity

5) Innovation

- Universality, Diversity and Innovation are not as specifically defined, but several initiatives in the spirit of these three are underway. These include increasing number of broadband and cellular subscriptions and the connection speeds thereof. Brazil had sought to reach an average broadband speed of 25 Mb/s by 2018, but it is behind on this goal as well as other infrastructural goals due to economic and political challenges [Arnaudo, 2016].

6) Neutrality of the network

- Net-neutrality refers to the equal treatment of all data on the internet. Under net-neutrality, networks do not discriminate based on content, source, nor destination.

7) Unaccountability of the network

- This refers to the concept that only the parties responsible for illicit activities on the internet should be targeted in combating their activities, rather than the “means of access and transport” [Arnaudo, 2016].

8) Functionality, security and stability

- Efforts to improve the security of Brazil's networks have often clashed with its privacy provisions. The aforementioned agencies have been created to combat cyber threats (mainly cybercrime). Brazil is hosting more international events, such as the Olympics in 2016, and expects to continue to do so in the future. Brazil is consequently preparing its law enforcement mechanisms to be able to deal with increased quantity of threats. Brazil has passed legislation calling for data localization in Brazil's internet in response to Snowden's leaks, but this is as far as Brazilian cybersecurity policy has gone [Arnaudo, 2016].

9) Standardization and interoperability

- Publicly available online databases should all be standardized and machine readable.

10) Legal and regulatory environments

- This refers to the principle of regulating the internet as a public resource, a core idea behind net-neutrality as well.

Brazil has not enacted any further legislation on cybersecurity since these were instituted, though there are still bills being debated in Brazil's Congress. However, it is likely that infrastructural changes will be a higher priority for Brazil. Accomplishing their data speed goals, for example, would be more beneficial politically than security measures that might conflict with the principles articulated

in MDI. Consequently, it will likely be a few more years before new meaningful cybersecurity policy gets passed in Brazil. They are, however, more empowered to counter cyber threats in the meantime.

India's Cybersecurity Policy

India instituted their National Cyber Security Policy in 2013. They are also expected to unveil an updated cybersecurity strategy in January of 2020 outlining budgetary requirements to accomplish their vision of a more secure cyber ecosystem [Bhalla, 2019]. Their current policy, like Brazil's and GDPR, prioritizes privacy and the protection of citizen's data. It also discusses cybersecurity extensively as a means to provide consumer confidence. The policy calls for a regulatory framework for mobile devices as well as creating incentives for technological innovation.

The strategies laid out are as follows, as per India's public information guide, Vikaspedia:

1) Creating a secure cyber ecosystem
    - This is intended to strengthen all entities involved in the cyber ecosystem. It is focused on information flow and technological development.
2) Creating an assurance framework

- This is intended to encourage the adoption of best practices by private firms and normalize methods of maintaining the practices.

3) Encouraging open standards
    - This is intended to improve interoperability between India's solutions and international solutions.
4) Strengthening the regulatory framework
    - This calls for a dynamic legal framework for handling cybersecurity concerns, especially as they arise from technological innovations.
5) Creating mechanisms for security threat early warning, vulnerability management and response to security threats
    - This calls for a 24x7 Computer Emergency Response Team to handle emerging cyber threats as well as plans for worst-case cyber scenarios.
6) Securing e-governance services
    - This encourages the use of Public Key Infrastructure (PKI) for government business and adopting best practices.
7) Protection and resilience of critical information infrastructure
    - This includes secure software development throughout its life cycle as well as creating a plan for protecting critical infrastructure.

8) Promotion of research & development in cyber security
    - This calls for cooperation between industry and academia in cybersecurity research among other goals for improving the research and development process.
9) Reducing supply chain risks
    - This calls for creating stronger relationships between vendors and a more robust supply chain closer to global standards.
10) Human resource development
    - This calls for greater education in cybersecurity.
11) Creating cyber security [sic] awareness
    - This calls for a creation of a national awareness program.
12) Developing effective public private partnerships
    - This refers to the domestic partnership between the government and private firms. It calls for the creation of a think-tank so that government and industry leaders can resolve cyber threats and determine how to adopt best practices.
13) Information sharing and cooperation
    - This refers to collaboration between law enforcement and national security agencies between countries.
14) Prioritized approach for implementation
    - This refers to implementing cybersecurity innovations in order of criticality.

In addition to this policy, India has a data privacy law called Reasonable Security Practices and Procedures and Sensitive Personal Data or Information. It was instituted in 2011 and required all organizations within India not to transmit sensitive data to any external third party that does not comport with the same data privacy rules [Brown, 2011]. In preparation for GDPR, India has been debating more updated data privacy laws. The most essential differences between GDPR and what India currently has is how third parties are defined to include domestic public entities as well (i.e. law enforcement) [Rodl & Partner, 2018]. India therefore has strong incentive to update their data privacy laws along with their updated cybersecurity policy.

China's Cybersecurity Policy

China's cybersecurity law, Network Security Act of the People's Republic of China (中华人民共和国网络安全法), does not specify network security standards. Rather, it gives the Chinese government a framework from which to draft additional cybersecurity policy and to create regulations for devices accessing any network within their territory. This comes in recognition of the fact that very specific standards and/or policies may need to be made in order to handle emerging vulnerabilities as they arise. This cannot generally be anticipated, so this strategy seems designed to reduce the reaction time to the discovery of a vulnerability through having the authority to require whatever is necessary.

The new law allows the Chinese government to regulate all aspects of network security except for military networks, which are handled by a separate ministry. The Chinese government will obtain information from “departments performing network security protection duties,” (Article 30) and this information must be used solely for the purpose of protection, as per the law. The law is sufficiently vague so that there are no clear limits other than that actions taken must be in the “societal public interest.” Article 39 discusses practices China might employ to resolve a threat or vulnerability which includes spot checks. Limits on what they can inspect, or demand access to, are not given.

The method of implementation for this law is not specified within its contents. It seems that the Chinese government is waiting to see how corporations operating in China become compliant with the precepts of the law and address difficulties as they arise. If this approach proves successful, it affords China a much more authoritative position to shape cyber norms. It remains to be seen which developing countries develop cybersecurity policies that are closer to the privacy focus of the Brazilian and Indian policies, closer to a both-and approach like India’s, or distinctly authoritarian like China’s.

In Sum

Data privacy is a core principle for Brazil and India’s approaches to cybersecurity. Stricter data privacy laws in the European Union are now pushing India to develop stronger data privacy laws to comply with GDPR as it is necessary for many of their businesses. However, India is not neglecting the

security side of cyber policy. Their 2013 law has established their essential strategy, but India will release a new cyber policy in January of 2020. Both Brazil and India have data privacy at their core, but India has shifted its focus in cyber policy to security recently. China's cybersecurity policy is distinctly authoritarian in making its security recommendations mandatory and having the right to any data needed to resolve a vulnerability or mitigate a threat.

Brazil's policy approach emphasized privacy and can encourage unbanked and underbanked citizens to adopt mobile payments to access financial services. Brazil is simultaneously empowering their law enforcement agencies and military to counter cyber threats more effectively rather than using a policy. India is updating their current cyber policy with ambitious goals. They already have a data privacy policy, but it is not as strict as GDPR, and they will likely need to update it. Fortunately, Indian companies are already working to become compliant with GDPR themselves, which should expedite the process for their development of a new data privacy policy.

These distinct policy approaches to cybersecurity might all be models other developing countries wish to follow. Whichever policies become most common could impact cyber norms significantly in the future.

Chapter 3: A Formalized Mechanism for Recommending Security Standards

Introduction

The Department of Homeland Security (DHS) released a report in 2017 to discuss its findings on the state of mobile device security and the implications for Government functions. It identifies significant needs in mobile infrastructure security and in the devices themselves. Importantly, it identifies two gaps in the ability of the DHS to address these issues:

1) Lack of authority in setting security requirements for mobile device carriers' mobile infrastructure
2) Lack of authority to demand information from carriers in order to assess security needs (though it can assess security based on what is provided voluntarily)

The report goes on to consider several possible actions to ameliorate the inability to respond to threats and vulnerabilities, all of which are designed to protect Government operations and development and, indirectly, protect consumers. Notably, it recommends that the Federal Government have a stronger presence

in bodies that develop security standards, a more robust public-private partnership, and that greater regulatory and legislative action be utilized to do so.

Also noteworthy is that the DHS report diverges in security priorities from the European Union's GDPR. It considers threats in the mobile space from the perspective of national security rather than consumer privacy protection. What DHS seeks is more akin to the intent of China's cybersecurity law than Brazil's, India's, or the European Union's. The relative positions of the United States and China in the world necessitate this sort of approach.

This work proposes a policy mechanism that can achieve the same level of security the DHS report seeks for mobile devices through a certification program whereby industry experts and Government agencies will contribute to a federally maintained set of requirements for mobile devices. Devices that conform to the standard prescribed in the set would be considered certified secure up to that standard. As a starting set, I propose implementing the 10 policies described in Cavallari et al and forcing software updates to be applied automatically within a definite timeframe. These standards would immediately improve the security of mobile devices with respect to financial data and conducting financial transactions. The details of these will be discussed in Chapter 6.

As is often quoted in discussions of cybersecurity, there exists no 'silver bullet' to resolve any category of software or hardware security vulnerabilities. It is a problem to be monitored and managed over time. There is no static list of

security measures that can resolve issues permanently because every innovation brings with it new vulnerabilities. Consequently, an effective policy approach must provide the flexibility needed to change the set of security requirements with relative speed. If there were broad authority provided to DHS or some other Federal Government agency to enforce requirements then this could still be expedient, but it would be more costly and carry with it some of the same concerns that apply to China's policy approach. It would require dedicated penetration testing to be carried out by a Federal Government agency or agencies to discover these issues and to resolve them. While many resources could be effective in discovering vulnerabilities, the makers of mobile device components are much better equipped to resolve them. Private organizations have utilized their own internal processes to do this as well as crowdsourcing through offering rewards for vulnerabilities private citizens identify. Private companies in the United States are not likely to support a measure that might require them to cede intellectual property or force them to consent to searches without warrants. It is preferable that they be provided an incentive to adopt security standards by means of a certification.

This approach can allow the United States to achieve the same level of security on mobile devices as it pertains to national security as China's policy. It creates additional incentives for creators of mobile devices, operating systems, and applications to make every effort to conform to the prescribed standards by making this a basis for competition. Currently, mobile devices compete on their

features. Data privacy is becoming a more common concern for consumers following significant breaches in the last few years. However, true device security is not currently something leading mobile device makers use to compete against one another. This work argues that this approach is likely to produce security outcomes that are at least as beneficial as what is possible with more centralized control over the process.

China's Ministry of Public Security (MPS) is ostensibly the organization that will be primarily conducting inspections and investigating vulnerabilities. In the United States, the approach is far more decentralized, wherein the creators of the components of mobile devices are responsible for improving their security. To illustrate the efficacy of this approach, in the 2017 WannaCry attack the vulnerability that the attack exploited was known to Microsoft, and a patch was created and distributed before the attack occurred. Unfortunately, some devices were not updated in time to be rendered invulnerable by the time the attack occurred. Nonetheless, the solution was developed and implementable before the attack occurred, showing a rapid response time.

Private technology companies often crowdsource investigating the vulnerabilities in their systems through "bug bounty" programs that offer private citizens rewards for what they discover. The United States Department of Defense (DoD) has also tried this approach with its own websites wherein it invited private citizens to seek vulnerabilities in its public-facing information systems so they could be resolved. The result was that 138 new vulnerabilities

were identified beyond what DoD had identified in its internal investigations. The program cost $150,000, amounting to roughly $1,100 per vulnerability [USDS, 2016]. DoD estimated that it would cost around $1 million to contract this work out to a cybersecurity firm. The results of this project further illustrate the benefit of a bottom-up approach over what might be projected for a top-down approach, wherein one organization is responsible for finding and fixing discovered vulnerabilities.

In addition to benefits to efficacy, this approach allows the United States to avoid the appearance of caprice more easily. The Federal Government recommends against private organizations utilizing foreign-developed hardware or infrastructure technology, such as the House Permanent Select Committee on Intelligence to Sprint in 2012 regarding Huawei and ZTE technology on its network. The report argued that since China's People's Liberation Army and Ministry of State Security had partially funded these two companies, they had an inappropriate competitive advantage over domestic technology companies [House Permanent Select Committee on Intelligence, 2012]. Furthermore, it found security vulnerabilities in the form of backdoors that could be used to transmit information back to China. Today, in the tense political relationship between China and the United States, China has argued that the United States is simply trying to advantage its own companies by removing foreign competition.

President Trump recently issued an executive order on Securing the Information and Communications Technology and Services Supply Chain on May

15, 2019. Shortly before that, the Five Eyes countries (The United States, The United Kingdom, Australia, New Zealand, and Canada) finally agreed to keep Huawei technology outside of their respective most sensitive networks. The United States took this measure further with the executive order in seeking to prohibit any sort of transaction that might harm national interests. China has claimed that this represents the United States attempting to disadvantage competition from China via security policy. The United States has traditionally maintained a distinction between economic and security policy. China has not. Both countries have powerful and opposing visions for cyber norms. The policy mechanism proposed in this work would exemplify this approach and give the United States a stronger hand in shaping global cyber norms through demonstrating the efficacy of its approach to cyber policy.

The Security Certification Program

The proposed program is a certification program whereby mobile devices that conform to a set of security standards will receive the certification. There are two types of criteria in this set: security requirements for the device and requirements for secure practices in the maintenance of the security of the operating system.

Worldwide, Android accounts for roughly 88% of all mobile operating systems while iOS accounts for roughly 11.8% (Statista, 2018). In the United States, the difference is much smaller. Android accounts for roughly 51% of all mobile operating systems while iOS accounts for 48.1%. No other mobile

operating system is anywhere close to either of these two worldwide, and so they will not be discussed. Since iOS is a closed operating system, it naturally does not have many of the vulnerabilities Android devices have. Additionally, the fact that Android accounts for a larger share of mobile operating systems domestically and a much larger share globally makes it the target of more attacks. Consequently, most of the device-layer recommendations listed as a starting set of criteria for this policy will be applicable to Android, while the practices will be applicable to all mobile device makers.

The core insight behind this list is that, as noted by Cavallari et al, while security updates and patches are often devised and distributed quickly, users can remove these changes or otherwise alter their device firmware such that it cannot receive these updates. Rooting or “jailbreaking” mobile devices can interfere with the security measures present in the device. While this already voids support from the device’s maker, it should also prevent the device from being able to participate in financial transactions. For any set of security requirements to be effective, it is necessary that none of them can be undone by the user or that if they are undone that the device is unable to make mobile payments. Though this will focus more on Android, this principle applies to iOS devices as well.

To achieve the goal of this program devices that do not meet the criteria for certification should not be able to participate in mobile payments. Roughly 44% of banking applications on the Apple App Store already attempt to detect if

the device is jailbroken and will not function if they detect it is. Unfortunately, detecting jailbreak or a rooted device is difficult. There are no certain tests for doing so on Android or iOS up to this point, and the methods the banking apps that do attempt this check utilize are mostly easy to defeat [Kellner et al, 2019].

Requirements

Under this certification program, I suggest as a starting point the following criteria be met to receive certification:

1) The device should utilize RootTools open source library to check “busybox,” “su,” and “root command” [Android]
2) The device should check the kernel’s build key; a value of “release-keys” for the “ro.build.tags” must be displayed. Alternative values indicate the kernel has been signed with third-party keys [Android]
    a. Note: this does not necessarily mean that the device has been rooted; it might indicate that the developer of the Android OS image did not properly sign it. If it is rooted, it will display “test-keys,” but the converse does not always hold.
3) The device should verify vendor certificates for over-the-air updates [Android]
4) The device should check for the presence of ids for developers that are known to develop rooting software [Android]
    a. Cavallari et al provides a recent list, but this would have to be monitored and updated.

5) The device should check for the presence of known applications and software known to be used in the rooting of devices [Android and iOS]
    a. Like the 4th item, Cavallari et al provides a list for Android and Kellner et al provides a partial list of iOS, but this would have to be monitored and updated.
6) The device should check for third party Android ROMs [Android]
    a. Legitimate device creators will use an official version of Android, so this is a good indicator that the operating system has been tampered with in some way.
    b. Again, Cavallari et al provides a list that would require monitoring and updating.
7) The device should check for the “su” binary in the locations provided by Cavallari et al; when found, execute the command and check the root permissions [Android]
    a. This is a tamper indicator; nothing in the user space should have access to root if there has been no tampering.
8) The device should check the permissions of the system folders, list provided by Cavallari et al [Android]
    a. None of the listed folders should even have read permissions; if they do, this is an indicator of tampering.
9) The device should check for the presence of BusyBox [Android]

    a. BusyBox is a utility that contains many tools that allow a user or malicious actor to tamper with Android.

10) The device should check for hidden files [Android]
    a. Cavallari et al suggest doing this by checking files with only execute permissions enabled.
11) Force updates within a defined timeframe [Android and iOS]
12) Prevent users from removing firmware [Android]
    a. On most Android devices this has been managed using Firmware Reset Protection. Samsung devices can have alternative firmware versions flashed onto them.
13) The device should prevent applications used to conduct financial transactions from running if the rest of the criteria are not met

Maintenance

To maintain this set, the requirements or policies added to it should satisfy the following three criteria:

1) Targeted at a specific security threat or vulnerability rather than the origin of hardware
2) Addressable by mobile device creators through patches or updated hardware in new devices
3) Solution and business-goal agnostic

These criteria ensure that in the maintenance of this set that requirements and policies are chosen based on their demonstrable security merits, that they are germane to the devices themselves, and that they are not designed to advantage any device creator over another.

Suggestions for Implementation

Cybersecurity is a problem to be managed rather than to be solved. This list is a beginning point, and its requirements will have to be updated and reviewed continually. Government, technology industry leaders, and retailers all have interests in the standards recommended by the policy. For the Government, having a mechanism to promote security policies necessary to protect Government operations and mobile infrastructure. For the technology industry leaders, it provides them a new method to gain market share. For retailers, it allows them to process customers more quickly and reduce fraud liability due to the significantly increased difficulty of compromising payments via mobile devices. This means that many groups of users have interest in maintaining global device security from different perspectives.

To merge these interests, the Security Certification Program should be managed by the Department of Homeland Security. Industry leaders, especially makers of mobile devices, and cybersecurity researchers would be the actors most able to detect security issues. The makers of mobile devices would be the most able to resolve security concerns on their respective devices. The Department of Homeland Security would provide the certification, but industry

leaders and researchers would advocate for the security standards and policies they believe would best counter emerging cyber threats. This would allow the United States to place requirements without having to disclose the details of why it is necessary when necessary.

Industry leaders, including both the technology companies that create mobile devices and those that create applications, technologies, and services with which they interact, would be important contributors to the set of requirements in this program. The instances of fraud experienced by retailers and restaurants would also be instructive as to new policies or requirements that need to be added to the set.

Compliance with the set could be checked with automated checks for the required settings each for Android and iOS (and any other operating system to which this becomes applicable in the future). This would simplify the process to demonstrate compliance so as to minimize the impact of procedural aspects of the program.

Security Advantages

In this section, this work argues that the approach of this program can accomplish the same levels of security as China's policy while still respecting intellectual property and privacy. It would also be less expensive than China's approach, operating through incentives instead of mandates. In particular, this approach incentivizes innovations in security from those best positioned to make

those innovations. Based on what was demonstrated by a Department of Defense program designed to resolve vulnerabilities in its public information system, crowdsourcing vulnerability detection is significantly less costly. This approach will also give the United States a more authoritative position to shape cyber norms, which would afford the United States a stronger position to advocate for international security policies that speak to the interests of the United States as they arise.

Centralized vs. Decentralized Approach

In 2016 the Department of Defense (DoD) received approval from the Pentagon to conduct a program dubbed “Hack the Pentagon.” The result of it demonstrated the efficacy of a distributed, decentralized approach to finding security vulnerabilities. Organizations as well as private citizens were invited to attempt to find vulnerabilities in the Department of Defense’s websites and information systems. This ‘bug bounty’ approach to security was novel for DoD. They contracted HackerOne, a bug bounty platform startup, to run the program, and DoD used their own digital services team and involved vendors to resolve the issues as they were found.

Noting that the estimated cost to hire a firm to perform the same task, the results were spectacular. A total of 138 vulnerabilities were found, all of which were missed by DoD’s own screening. The very first vulnerability report was received in only 13 minutes. Over 1,000 individuals participated in the program and the total cost for the program, including what was payed out in bounties and

the resolution of the vulnerabilities, was roughly $150,000. The cost to hire a firm to find and resolve these was estimated at over $1,000,000.

The impressive result of this program has prompted DoD to implement more such programs. Other government agencies and stakeholders are also considering the decentralized approach of crowdsourcing the finding of vulnerabilities. The clearest contrast that can be drawn between the decentralized approach and the centralized approach is the difference in the cost. However, a priori, a decentralized approach has additional advantages as well.

The first advantage is the potential to draw on a broad knowledge base with many specialties and perspectives. In a centralized approach, either with a single contractor or with a single government agency being responsible for finding and resolving security threats, the knowledge base is restricted to the agency or organization. Offering bounties to individuals is less expensive than formally contracting the work out or paying other employees to perform the task. Of course, crowdsourcing is not a replacement for an organization's own inspection of their products or services. It is, however, a very helpful addition.

Technology companies frequently utilize bug-bounties and the crowdsourcing approach to find bugs and vulnerabilities in their systems. Under this certification program, this advantage would be maintained insofar as makers of mobile devices continue to utilize the crowdsourcing approach in addition to

their own processes. Any contributor with a meaningful innovation or insight could improve the overall state of mobile device security.

Comparison to Plastic Cards

Plastic cards are significantly less secure than mobile devices for mobile payments. The main source of this insecurity is the medium itself. A plastic credit card has all or nearly all of the information required to make a payment, depending on if a zip code is required. This means a stolen card is immediately available to be used to make a payment. This is not true for mobile devices; Apple Pay, Google Pay, and Samsung Pay, which do not store credit card information on the devices themselves.

Mobile payments in the United States generally use Near-Field Communication (NFC) to make the transaction. In the case of mobile wallets, which account for the majority of mobile payments, the user connects a credit or debit card to their mobile wallet. Depending on the service, the user might enter a pin or use their fingerprint when they initiate the transaction. From the user's perspective, this is all they need to do. With Apple Pay, the user uses their fingerprint or face to validate the transaction. With Google Pay, the user simply needs to unlock the device (which can be done with fingerprint, face, or pin).

With Apple Pay the generated token is stored in a Secure Element (SE) chip, which then generates a cryptogram. The merchant sends the request to their bank, which then forwards the request to the payer's bank or payment

provider. Since what was transmitted is not a true account number but rather a reference to one, the payment network will send it on to the token service provider (typically a third-party vendor), who will then provide the true account number. This then means that payment provider can authorize or deny the transaction and send the notification back to the merchant. Google Pay is quite similar; the essential difference is that instead of using a physical SE chip in the phone it uses Google's own cloud servers. The security tradeoff is that there is less risk from a lost or stolen device but there is more risk due to real card data being stored in Google's cloud servers. The phone itself thereby emulates a physical card by means of that tap. However, in both approaches, even if a hacker or malicious actor intercepts the information transmitted in the transaction, they are not able to glean the card number, the account to which it is tied, nor any other personally identifiable information (PII). This makes mobile payments significantly more secure than plastic cards, where a lost or stolen card can immediately be used for a fraudulent transaction.

Chip cards have been effective in reducing fraud from in-person payments as they are very difficult to counterfeit compared to magnetic strips. According to Visa, instances of fraudulent payments caused by counterfeiting plastic cards had dropped by 82% since the adoption of chip cards in 2015 and November of 2018. Chip cards essentially utilize the same tokenization strategy as mobile payments. The differences in their security come from the use of the card itself.

Stolen cards present a much bigger security challenge than stolen devices. This is because card-not-present (CNP) transactions are still possible and easy to do with a stolen card. With a stolen mobile device, it is much harder. At a minimum, the device must be unlocked. The card information linked to the mobile wallet is not stored on the actual phone, further limiting the ability to commit fraudulent payments with a stolen device. Furthermore, Android and iOS devices both have functionality to erase all data and/or render the device unusable to whomever stole it. These measures create layers of security beyond the transaction itself and make mobile Point-of-Sale (PoS) a distinctly more secure payment tool.

Due to current levels of adoption of mobile payments in the United States, there is insufficient data to make a meaningful comparison between the instances of fraud between the two. In a few years this will be clearer, but from the available information, the instances of fraudulent payments from plastic cards should be greater than the number from mobile payments.

In addition to security, the mobile payments are quicker for a user to enter. This is because with chip cards the card must remain inserted while the transaction is being processed, whereas with a mobile device the user is finished as soon as they have tapped it.

Global Cyber Norms

The term ‘cyber norms’ refers to the notions of the acceptable use of cyberspace. At present, cyber weapons as well as the massive amounts of user data in the internet ecosystem have posed new questions about what is appropriate in cyberspace and what is not. Data privacy concerns have been at the forefront of normative thinking with states implementing policies targeted toward protecting consumer data. However, several other normative questions remain. Stuxnet illustrated that cyber attacks could be used effectively to carry out objectives that previously required a kinetic operation. Unlike other non-conventional weapons like nuclear arms, global powers tend to keep their true capabilities secret with respect to weapons. Another set of norms in cyberspace is the set surrounding what is acceptable for security policy.

Fortunately, for this last set, this certification program could help the United States define this more formally. The United States has derided China for using its security policy to accomplish economic goals. Huawei, the Chinese technology giant, receives significant funding from the People’s Liberation Army, China’s National Security Commission, and an additional Chinese intelligence agency, according to the Central Intelligence Agency [Doffman, 2019]. The United Kingdom’s Huawei Cyber Security Evaluation Centre has claimed that it also found issues that were sufficiently concerning to them that they do not believe they can safely include Huawei technology in networks in the United Kingdom while maintaining their own domestic network security.

Initially, the Five-Eyes countries were not as quick to make pronouncements following the claims of the United States about the risks of incorporating Huawei technology on domestic networks. However, the apparent confirmation of the funding relationship between Chinese intelligence and Huawei was compelling, as this violates a norm of abstaining from using security policy for economic advancement. With the initial claims from the United States, it was possible to infer a motive related to the trade war between the United States and China. However, upon more information becoming available, the normative logic of preserving a distinction between security interests and economic interests in security policy made the decision obvious.

The United States having a formal policy mechanism will make avoiding such an appearance easier. The criteria provided for what requirements can be included in the policy prevent a blanket ban on Huawei technology, but it does not prevent excluding it on the basis of the presence of a backdoor, which is the specific security concern associated with this issue.

Business Interests

In addition to the security benefits of this policy, there are incentives for retailers and restaurants as well as technology companies and makers of mobile devices to support this policy. Retailers stand to benefit through less expected cost for fraud liability and the ability to process consumer payments faster. Technology companies will have a greater platform for their security innovations

and the makers of mobile devices will be able to compete on the basis of security.

Retailers

A consequence of the security benefits of mobile devices is that though the fraud liability is the same as it would be for plastic cards the expected amount of fraud is less. These benefits reduce the overall risk to retailers and restaurants of having to cover these costs. Reduced costs could in turn allow retailers to reduce their prices and stimulate demand. This also helps to offset the cost of adopting the technologies needed to facilitate point-of-sale technology. Retailers and Restaurants have already adopted these technologies to a large extent. Given this, it is in the interest of retailers and restaurants for users to continue to increase their utilization of mobile payments and that there be a mechanism to standardize their security requirements and policies. This would continue to minimize instances of fraud and thereby their exposure to fraud liability.

With respect to in-person card-present transactions, restaurants and retailers can be held liable for fraud if they process a transaction that they believe to be fraudulent, fail to require a chip card, or fail to require a signature. They are empowered to require identification and to inspect the card being used to prevent a fraudulent transaction. With mobile devices, the layers of security should continue to keep the amount of fraud less than what has occurred by cards. Therefore, their overall expected cost will be lower.

Technology Companies

Technology companies that do not create mobile devices would have a significant role to play in the certification program. Cybersecurity firms and companies that develop the technologies, apps, or services with which mobile devices interact would all be vital players in identifying security concerns that may need to be addressed. They would have an additional platform to advocate for their cybersecurity innovations and they could use their innovations as a basis for competition and thereby an avenue to increase their market share.

In Sum

The proposed certification program is a policy mechanism that would allow the United States to manage cybersecurity threats and vulnerabilities as they arise. An initial set of requirements was provided designed to target prerequisites for known attacks to compromise mobile device transaction security. The certification program would fulfill some of the needs identified in the Department of Homeland Security's Study on Mobile Device Security in providing a formal mechanism for industry leaders and Government to ensure that security policy caters to the needs they both identify with respect to device security.

It may remove other needs the report identified by rendering the need for additional regulatory authority unnecessary. If the makers of mobile devices are sufficiently incentivized to maintain certification for their devices, or to create new

devices that are certified, then there is no need for a more authoritative hand. This is much more politically feasible while achieving the same levels of security.

There are several security advantages to this approach. Mobile devices are more secure than plastic cards and having a formal security mechanism might help to improve consumer confidence in their security. Contrasting it with China's cybersecurity policy's centralized approach, this policy would likely allow the United States to find and resolve security concerns at least as efficiently as China's policy. It would also preserve the traditional normative distinction between pursuing security interests and economic interests in cybersecurity policy. This would give the United States a more authoritative position to shape global norms going forward, as there are still several open questions about the acceptable use of cyberspace.

Conclusion

This work presents a policy mechanism for the United States to manage cybersecurity vulnerabilities and threats on mobile devices. Current trends in adoption of mobile payments in the United States indicate that mobile payments are likely to be a main form of payment in the near future. This makes the need to develop a cybersecurity policy for mobile devices more urgent. In addition to the utilization of mobile devices by consumers, the Department of Homeland Security's (DHS) Study on Mobile Device Security identified the need for greater ability to manage mobile device security to protect Government operations. It also called for increases in the public/private partnership between industry leaders and the DHS and giving DHS greater regulatory authority in resolving security concerns.

Given these motivations, this work proposes a certification program be created whereby a set of criteria for certification must be met by a device for the device to be certified. The criteria would be based on best practices and the most recent discoveries in device vulnerabilities. A suggested set of criteria to begin this program is provided. These are based on recent research into removing the security innovations mobile device creators push or being able to execute code at a higher level of privilege than should be possible through rooting or

jailbreaking the device. Detecting rooting or jailbreaking is a challenging task but vital to device security. The list includes several methods for detecting if an Android device is rooted. Jailbreak detection is similarly challenging on iOS and current app-based methods for doing so have proven to be easily defeated. Consequently, this is an essential target for the certification program.

To maintain the program, three criteria should be met for new requirements or policies to be added. The requirements or policies should be:

1) Targeted at a specific security threat or vulnerability rather than the origin of hardware
2) Addressable by mobile device creators through patches or updated hardware in new devices
3) Solution and business-goal agnostic

These criteria preserve the advantages of this policy approach over China's approach, including a decentralized approach to discovering security vulnerabilities, strong incentives for industry leaders to contribute actively, and no additional mandates or legal requirements imposed on the private sector.

While mobile device security is certainly taken seriously in the United States both by technology companies and by the Government, there is often misalignment in the problems they each seek to solve. Consequently, a program over which the Government has final say in certification but where no legal requirements are imposed optimizes the ability to develop solutions that cater to

both sets of goals. For businesses, consumer protection and market share are always underlying incentives. For governments, ensuring the safety and integrity of operations is vital to their missions. In the consumer market, being able to guarantee a minimum level of security across all devices that conduct transactions is advantageous to both goals.

Technology companies tend to utilize programs like bug bounties to resolve cybersecurity concerns. This has proven to be a cost-efficient addition to internal security evaluations, both for technology companies and for governments. The Hack the Pentagon program put on through the Department of Defense was able to find 138 additional vulnerabilities for roughly 15% of the cost of hiring a single firm to perform the same task. This illustrates the efficacy of the decentralized approach. This can be achieved through the certification program, where many entities are involved in finding vulnerabilities, but not in the centralized approach of China.

Business interests would be well served by this policy approach as well. Retailers and restaurants can be held liable for fraudulent transactions that occur in their establishments if they fail to follow procedures set forth by payment card providers. While chip cards have reduced these instances dramatically over what was seen with simple magnetic strip cards, they have not eliminated them, and are still much easier to compromise than smartphones. The physical card itself can be used immediately in most cases if stolen, which is not true for a mobile device, which must be unlocked at a minimum to be of use for payments. For the

makers of mobile devices, this provides an additional avenue for competition and therefore increased opportunity to grow market share.

The BRIC countries have seen particularly spectacular growth in mobile device and mobile payment adoption. China represents a mature state of mobile payments being used as a primary tool of consumption. India is the fastest growing mobile payments market in the world, and Brazil is preparing for a similarly impressive increase in mobile device utilization for payments. They have each implemented cyber policies based on their specific needs and geopolitical positions. China's is focused on security with little regard for privacy, India is incorporating both, and Brazil is distinctly privacy-focused from a policy perspective. As all of these countries work to position themselves to counter state-level cyber activities as well as criminal level, they will have to incorporate more security-specific policy.

The United States, like China, must be focused on security in its cyber policy as well. It represents the largest economy in the world as well as a global hegemon. Consequently, it must focus both on cybercrime as well as state-based cyber threats. This policy allows the United States to do so effectively and will allow it to continue to do so as cyberspace evolves.

Future Work

From a policy perspective, while this policy can accomplish improved minimum standards for mobile device security, it does not solve the regulatory concerns the DHS report voiced over mobile networks. The approach presented here is not well suited for this task, but it is also necessary.

From a cybersecurity perspective, the methods for two-factor authentication are less effective than in other applications. Biometrics ('something you are') has the disadvantage of being unchangeable but can be just as compromised as a password in a digital form. If a malicious actor has the device and the password, two-factor authentication methods that send an SMS message as well as requiring a password are no more secure than single-factor authentication. This makes two-factor authentication significantly less useful on mobile devices and some improved methods would be welcome additions.

Bibliography

1. "Identifying Security Vulnerabilities in Department of Defense Websites – Hack the Pentagon." usds.gov, The United States Digital Service, 2016.
2. "US Proximity Mobile Payment Users, by Platform, 2018 (millions)." , eMarketer, 1 May 2018.
3. C.S. "Why Americans are warming to mobile payments." , Economist, 18 June 2018.
4. eMarketer, and AP. "Number of Mobile Phone Users in Brazil from 2013 to 2019 (in Millions)." Statista, Statista Inc., 31 Aug 2015, https://www-statista-com.du.idm.oclc.org/statistics/274695/forecast-of-mobile-phone-users-in-brazil/
5. Sengupta, Hindol. "India’s ₹1 trillion mobile payment system." fortuneindia.com, Fortune, 5 Jan. 2019.
6. Pang, Jeffrey, et al. "Challenges in Mobile Security." , DSTA Horizons, 2016.
7. Wildau, Gabriel, and Leslie Hook. "China mobile payments dwarf those in the US, research shows." Financial Times, Financial Times, 13 Feb. 2017. Accessed 6 Apr. 2017.
8. "Chip technology has helped reduce card-present counterfeit payment fraud by 82 percent." usa.visa.com, Visa, 27 Nov. 2018.
9. "Executive Order on Securing the Information and Communications Technology and Services Supply Chain." whitehouse.gov, The White House, 15 May 2019.

10. "Indian Data Privacy laws and EU GDPR." roedl.com, Rodl & Partner, 24 May 2018.
11. "Payment methods in China: How China became a mobile-first nation." daxueconsulting.com, Daxue Consulting, 10 May 2019.
12. "The Intersection Of Payments And Commerce In A Digital World." , Forrester Research Inc., Feb. 2017.
13. Arnaudo, Daniel. "Brazil, the Internet and the Digital Bill of Rights." https://igarape.org.br/, Igarape Institute, 2016.
14. Bhalla, Kritti. "India To Get National Cybersecurity Policy By January 2020." inc42.com, Inc42, 29 Aug. 2019.
15. Boston Retail Partners. "Digital Payment Methods That North American Retailers Accept or Plan to Accept as of December 2018." Statista, Statista Inc., 18 Jan 2019, https://www-statista-com.du.idm.oclc.org/statistics/384921/digital-payment-methods-retail-america/
16. Brown, Peter. "New Indian Privacy Law Impacts U.S. Companies." dataprivacymonitor.com, Data Privacy Monitor, 29 July 2011.
17. Cavallari, Maurizio, et al. "Innovative Security Techniques to Prevent Attacks on Wireless Payment on Mobile Android OS." , Springer Nature Singapore Pte Ltd., Jan. 2019.
18. comScore. "Subscriber Share Held by Smartphone Operating Systems in The United States from 2012 to 2019." Statista, Statista Inc., 30 Aug 2019,

https://www-statista-com.du.idm.oclc.org/statistics/266572/market-share-held-by-smartphone-platforms-in-the-united-states/

19. Deloitte. (2016). 2016 Global mobile consumer survey: US edition. From https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-global-mobile-consumer-survey-2016-executive-summary.pdf
20. Deloitte. (2018). 2018 Global mobile consumer survey: US edition. From https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-global-mobile-consumer-survey-exec-summary-2018.pdf
21. Dimitriadis, Christos. "CSX Mobile Payment Security: Perceptions and Behaviors." isaca.org, ISACA, 2015.
22. Doffman, Zak. "CIA Claims It Has Proof Huawei Has Been Funded By China's Military And Intelligence." Forbes.com, Forbes, 20 Apr. 2019.
23. FireEye Inc & Madinant, Inc., 2014. “Cybersecurity’s Maginot Line: A Real-World Assessment of the Defense-in-Depth Model”
24. Frey, William. "The millennial generation: A demographic bridge to America’s diverse future." brookings.edu, Brookings, Jan. 2018.
25. Fry, Richard. "Millennials projected to overtake Baby Boomers as America’s largest generation." pewresearch.org, Pew Research Center, 1 Mar. 2018.
26. Gartner. "Global Mobile Os Market Share in Sales to End Users from 1st Quarter 2009 to 2nd Quarter 2018." Statista, Statista Inc., 28 Aug 2018,

https://www-statista-com.du.idm.oclc.org/statistics/266136/global-market-share-held-by-smartphone-operating-systems/

27. Gochhwal, R. (2017) Unified Payment Interface—An Advancement in Payment Systems. American Journal of Industrial and Business Management, 7, 1174-1191.
28. Griffith, Dr. Robert P. Study on Mobile Device Security. U.S. Department of Homeland Security, 2017.
29. Holm, Orjan, et al. "A Study of Mobile Payment Behavior in Four Countries." International Journal of Business and Information, vol. 13, no. 3, Sept. 2018, p. 349-384.
30. Islam, Ali, et al. "SMB Exploited: WannaCry Use of "EternalBlue"." fireeye.com, FireEye Inc, 2017.
31. Kats, Rimma. "The Mobile Payments Series: India." emarketer.com, eMarketer, 5 Nov. 2018.
32. Kellner, Angsgar, et al. "False Sense of Security: A Study on the Effectivity of Jailbreak Detection in Banking Apps." , Institute of System Security, TU Braunschweig, Aug. 2019.
33. Leandro Bolzan de Rezende, Paul Blackwell & Marcos Degaut (2018) Brazilian National Defence Policy: foreign policy, national security, economic growth, and technological innovation, Defense & Security Analysis, 34:4, 385-409, DOI: 10.1080/14751798.2018.1529084
34. Rafter, Dan. "Android vs. iOS: Which is more secure?" , Symantec, 2019.

35. Rogers, Mike, and Dutch Ruppersberger. "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE." , House Permanent Select Committee on Intelligence, 8 Oct. 2012.
36. Visa Innovation Center, 2019. “The state of innovation in Latin America: Lessons from innovative companies across the region”
37. Website (paymentscardsandmobile.com). (n.d.). Mobile payments in the United States from 2014 to 2019, by segment (in million U.S. dollars). In Statista - The Statistics Portal. Retrieved June 12, 2019, from https://www.statista.com/statistics/312492/mobile-payments-in-the-united-states-by-segment/.
38. Weiss, Brett, "An Investigative Study on Android Verified Boot Process" (2019). Creative Components. 278
39. World Bank. "Share of Adult Population with a Bank or Mobile Money Service Account in Brazil between 2011 and 2017." Statista, Statista Inc., 19 Apr 2018, https://www-statista-com.du.idm.oclc.org/statistics/898974/population-bank-account-type-brazil/